

# PRODUCT-FREE SUBSETS OF PROFINITE GROUPS

MOHAMMAD BARDESTANI AND KEIVAN MALLAHI-KARAI

**ABSTRACT.** Gowers in his paper on quasirandom groups studies a question of Babai and Sos asking whether there exists a constant  $c > 0$  such that every finite group  $G$  has a product-free subset of size at least  $c|G|$ . Answering the question negatively, he proves that for sufficiently large prime  $p$ , the group  $\mathrm{PSL}_2(\mathbb{F}_p)$  has no product-free subset of size  $cn^{8/9}$ , where  $n$  is the order of  $\mathrm{PSL}_2(\mathbb{F}_p)$ .

We will consider the problem for compact groups and in particular for the profinite groups  $\mathrm{SL}_k(\mathbb{Z}_p)$  we obtain lower and upper exponential bounds for the supremal measure of the product-free sets. The proof involves establishing a lower bound for the dimension of non-trivial representations of the finite groups  $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$ .

## 1. INTRODUCTION

Let  $G$  be a finite group. One can then ask how large a subset  $A$  of  $G$  can be so that the equation  $xy = z$  has no solution in  $A$ . The precursor of all the results in this direction, due to Erdős, states that a finite subset  $X$  of the additive group of integers  $\mathbb{Z}$  has always a sum-free subset of size at least  $|X|/3$ . Even though the result involves an infinite group, it can be easily seen to be equivalent to the analogous statement where  $\mathbb{Z}$  is replaced by  $\mathbb{Z}/(p\mathbb{Z})$  for a large enough prime  $p$ .

Gowers in his paper on quasirandom groups [6] studies a question of Babai and Sos [2] asking whether there exists a constant  $c > 0$  such that every finite group  $G$  has a product-free subset of size at least  $c|G|$ . Answering the question negatively, he proves that for sufficiently large prime  $p$ , the group  $\mathrm{PSL}_2(\mathbb{F}_p)$  has no product-free subset of size  $cn^{8/9}$ , where  $n$  is the order of  $\mathrm{PSL}_2(\mathbb{F}_p)$ . Behind this result lies the fact that  $\mathrm{PSL}_2(\mathbb{F}_p)$  has no nontrivial irreducible representations in low dimensions. The same property has been used by Lubotzky, Phillips and Sarnak [13] to show that the Ramanujan graphs are expanders. Later Bourgain and Gamburd [4] also used this to prove that the Cayley graphs of  $\mathrm{SL}_2(\mathbb{F}_p)$  form a family of expanders. Gowers' theorem, apart from its intrinsic interest, have some important applications. Indeed Nikolov and Pyber [14], by using Gowers' theorem, have obtained improved versions of recent theorems of Helfgott [8] and of Shalev [16] concerning product decompositions of finite simple groups.

In this paper we will consider similar problems for compact groups. Let  $G$  be a compact, Hausdorff, second countable topological group and  $\mu$  denote the Haar measure on  $G$ , normalized so that  $\mu(G) = 1$ . Note that since  $G$  is compact, and hence unimodular, a left Haar measure is automatically right invariant. A measurable subset of  $A$  is said to be product-free if  $A^2 \cap A = \emptyset$ . Let  $\mathrm{pf}(G)$  denote the supremum of  $\mu(A)$  where  $A$  runs over all product-free measurable subsets of  $G$ .

---

2010 *Mathematics Subject Classification.* 20P05, 20F, 20C33.

*Key words and phrases.* Profinite group, Complex representation, Hilbert-Schmidt operator, Singular value decomposition .

A special class of compact groups that will be studied in this paper are profinite groups. A compact group  $G$  is profinite if it is the projective limit of finite groups. The question of establishing lower and upper bounds for  $\text{pf}(G)$  is natural for many classes of groups. Let  $\text{SU}_n$  be the special unitary group on  $\mathbb{C}^n$ . Gowers [6] asked if  $\text{pf}(\text{SU}_n) < c^n$  for some  $c < 1$ . The available methods only give polynomial bounds for these groups. On the other hand, for profinite groups, using their close connection to the finite groups, we can establish exponential lower and upper bounds.

In this paper, after introducing the notion of product-free measure of a compact group, we will show that for abelian groups the exact value of the product-free measure can be explicitly computed. More precisely we will prove

**Theorem 1.** *The product-free measure of the additive groups of  $p$ -adic integers  $\mathbb{Z}_p$  and power series  $\mathbb{F}_p[[t]]$  are respectively given by,*

$$(1) \quad \begin{aligned} \text{pf}(\mathbb{Z}_p) &= \begin{cases} 1/3 + 1/(3p) & \text{if } p \equiv 2 \pmod{3} \\ 1/3 & \text{otherwise} \end{cases} \\ \text{pf}(\mathbb{F}_p[[t]]) &= \begin{cases} 1/3 + 1/(3p) & \text{if } p \equiv 2 \pmod{3} \\ 1/3 & \text{if } p = 3 \\ 1/3 - 1/(3p) & \text{if } p \equiv 1 \pmod{3} \end{cases} \end{aligned}$$

The main part of this paper is devoted to obtaining upper bound for  $\text{pf}(G)$ . In order to obtain such bound, we will prove the following

**Theorem 2** (Mixing inequality). *Let  $G$  be a compact, Hausdorff, second countable topological group such that any non-trivial complex continuous representation of  $G$  has dimension at least  $\ell$ . Let  $f_1, f_2 \in L^2(G)$  and at least one of the  $f_1, f_2$  belongs to  $L_0^2(G)$ . Then*

$$(2) \quad \|f_1 * f_2\|_2 \leq \sqrt{\frac{1}{\ell}} \|f_1\|_2 \|f_2\|_2.$$

Babai, Nikolov, and Pyber [1] proved this inequality for finite groups. This generalization integrates ideas from the previous works with tools and concepts from functional analysis.

**Corollary 1.** *Let  $G$  be a compact, Hausdorff, second countable topological group such that any non-trivial complex continuous representation of  $G$  has dimension at least  $\ell$ . Let  $A, B \subseteq G$  be two measurable sets then*

$$(3) \quad \|1_A * 1_B - \mu(A)\mu(B)\|_2 \leq \sqrt{\frac{\mu(A)\mu(B)}{\ell}}$$

For compact groups we can establish the following analogue of Gowers' Theorem [6]:

**Theorem 3.** *Suppose  $G$  is a compact, Hausdorff, second countable topological group such that any non-trivial complex continuous representation of  $G$  has dimension at least  $\ell$ . If  $A, B, C \subseteq G$  such that  $\mu(A)\mu(B)\mu(C) > \frac{1}{\ell}$  then the set  $AB \cap C$  has positive measure. Moreover, if  $\ell\mu(A)\mu(B)\mu(C) \geq \frac{1}{\eta^2}$  then*

$$(4) \quad \mu\{(x, y, z) \in A \times B \times C : xy = z\} \geq (1 - \eta)\mu(A)\mu(B)\mu(C).$$

In order to obtain explicit upper bounds for product-free measure of the groups  $\mathrm{SL}_k(\mathbb{Z}_p)$ , we will need to establish a lower bound for the dimension of the non-trivial complex continuous representations of these groups. As  $\mathrm{SL}_k(\mathbb{Z}_p)$  is profinite, the problem immediately reduces to the representations theory of all finite quotients. We will then generalize the already known bounds for the finite almost simple group  $\mathrm{SL}_k(\mathbb{Z}/(p\mathbb{Z}))$  the extensions  $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$  of these groups. Our method is quite elementary compared to the work of Landazuri and Seitz paper [12] where they obtain, among other things, the minimal dimension of non-trivial representation of  $\mathrm{PSL}_k(\mathbb{F}_p)$ . This inequality is interesting in its own right.

**Theorem 4.** *The minimum dimension  $m(p, k)$  of all non-trivial complex continues representation of the group  $\mathrm{SL}_k(\mathbb{Z}_p)$  satisfies:*

$$(5) \quad \begin{aligned} m(p, k) &\geq p^{k-1} - p^{k-2} \quad \text{for } k \geq 3, \\ m(p, 2) &\geq \frac{p-1}{2}. \end{aligned}$$

**Remark 1.** As we are interested only in the asymptotic behavior of  $\mathrm{pf}(\mathrm{SL}_k(\mathbb{Z}_p))$  we did not make any attempt to find the optimal bound, which is likely to be  $p^{k-1} - 1$  for all  $k \geq 3$ .

A lower bound for  $\mathrm{pf}(\mathrm{SL}_k(\mathbb{Z}_p))$  can be obtained by considering a particular maximal parabolic subgroup of small index. Combining the main theorem with the lower bound, we obtain the following bounds for  $\mathrm{pf}(G)$ :

**Theorem 5.** *Fix a prime number  $p > 2$ . Then the product-free measure of the special linear group  $\mathrm{SL}_k(\mathbb{Z}_p)$  decays exponentially with  $k$ . More precisely,*

$$(6) \quad \begin{aligned} \frac{p-1}{p^k-1} &\leq \mathrm{pf}(\mathrm{SL}_k(\mathbb{Z}_p)) \leq \frac{1}{(p^{k-1} - p^{k-2})^{1/3}}. \\ \frac{1}{p+1} &\leq \mathrm{pf}(\mathrm{SL}_2(\mathbb{Z}_p)) \leq \left(\frac{2}{p-1}\right)^{1/3}. \end{aligned}$$

Combining Theorem 3 and 5 we have:

**Corollary 2.** *If  $A$  is a measurable subset of  $\mathrm{SL}_k(\mathbb{Z}_p)$  with*

$$(7) \quad \begin{aligned} \mu(A) &> \frac{1}{(p^{k-1} - p^{k-2})^{1/3}} \quad \text{for } k \geq 3, \\ \mu(A) &> \left(\frac{2}{p-1}\right)^{1/3}, \end{aligned}$$

*then  $A^3 = G$ .*

**Proof:** Let  $k \geq 3$ . For every  $g \in G$ , set  $B = A$  and  $C = gA^{-1}$ . Since

$$\mu(A)\mu(B)\mu(C) = \mu(A)^3 > \frac{1}{(p^{k-1} - p^{k-2})},$$

then by Theorem 3 and Theorem 4,  $AB \cap C \neq \emptyset$ . If  $x \in AB \cap C$  then  $x = ga_3^{-1} = a_1a_2$  for  $a_1, a_2, a_3 \in A$  which proves the claim. Proof is similar for  $k = 2$ .  $\square$

**Remark 2.** It is noteworthy that the same methods can be used to get similar bounds for  $\mathrm{SL}_k(\mathbb{F}_p[[t]])$ . We can also obtain similar bounds for certain classes of Chevalley groups. These results will appear elsewhere.

Using a similar method, we will obtain lower and upper bounds for the subgroup  $A_{k+1}^+$  of positive automorphism group of a rooted regular tree. For the definition of this subgroup we refer the reader to Section 8.

**Theorem 6.** *For all  $k \geq 5$  we have*

$$(8) \quad \frac{1}{k+1} \leq \mathrm{pf}(A_{k+1}^+) \leq \frac{1}{(k-\epsilon)^{1/3}}.$$

where  $\epsilon = 0$  if  $k$  is even and  $\epsilon = 1$  when  $k$  is odd.

This paper is organized as follows: In Section 2 we will recall some definitions and set the notations. In Section 3 we establish some elementary properties of  $\mathrm{pf}(G)$  and give a proof of Theorem 1. In Section 4 and Section 5 we gather some facts about the representation theory of profinite groups. Gowers' proof [6] uses the language of quasirandom graphs. We will translate his argument to direct arguments in functional analysis involving Hilbert-Schmidt operators which is more suitable for the compact groups. This is done in Section 6. In Section 7 and 8 we will prove Theorems 3, 5, 6 which are the main results of this paper.

## ACKNOWLEDGMENT

We have benefited from some notes on Terence Tao's weblog as well as Emmanuel Breuillard's lecture notes on "Théorie des groupes approximatifs". We wish to thank them for providing these notes online. For many fruitful discussions, we wish to thank Andrew Granville. The first author was supported in part by Faculté des Études Supérieures et Postdoctorales de l'Université de Montréal. The second author would like to thank CRM in Montreal for the visit during which part of this joint work was done.

## 2. PRELIMINARIES AND NOTATIONS

Groups considered in this paper are assumed to be compact, Hausdorff and second countable. In general the group operation is denoted multiplicatively; we occasionally make an exception for abelian groups and shift to the additive notation. We use  $\mu$  for the normalized bi-invariant measure on the group. The corresponding Lebesgue spaces will be denoted by  $L^p(G)$  and the respective norm is denoted by  $\|\cdot\|_p$ . For a subset  $A$  of a group  $G$ , we use  $1_A$  to denote the characteristic function of  $A$ . For subsets  $A$  and  $B$ , the product set  $AB$  is the set of all products of the form  $ab$  where  $a \in A$  and  $b \in B$ . We also use  $A^2 = AA$ . The cardinality of a finite set  $A$  will be denoted by  $|A|$ . The finite field with  $p$  elements is denoted by  $\mathbb{F}_p$ .

We will be working with the ring of  $p$ -adic integers and the ring of formal power series over  $\mathbb{F}_p$ , denoted respectively by  $\mathbb{Z}_p$  and  $\mathbb{F}_p[[t]]$ . Each one of these groups is equipped with the profinite topology.

Profinite groups are defined as the projective limits of finite groups. Let  $I$  be a directed partially ordered set. Consider a sequence of finite groups  $\{G_i\}_{i \in I}$  and homomorphisms  $\phi_{ij} : G_j \rightarrow G_i$  for

all  $j \geq i$ , such that  $\phi_{ii} = \text{id}_{G_i}$  and  $\phi_{kj}\phi_{ji} = \phi_{ki}$  for all  $k \geq j \geq i$ . One can then define the projective limit of  $\{G_i\}$  which is a profinite group denoted by  $\varprojlim G_i$ .

Of special interest is when  $G_i$  is the finite cyclic groups  $\mathbb{Z}/(p^i\mathbb{Z})$  and for  $j \geq i$  the map  $\phi_{ji} : \mathbb{Z}/(p^j\mathbb{Z}) \rightarrow \mathbb{Z}/(p^i\mathbb{Z})$  is reduction modulo  $p^i$ . The projective limit which is denoted by  $\mathbb{Z}_p$  is the additive group of  $p$ -adic integers. One obtains a natural projections  $\phi_i : \mathbb{Z}_p \rightarrow \mathbb{Z}/(p^i\mathbb{Z})$ . Note that  $\mathbb{Z}_p$  constructed in this way has also a ring structure. A similar construction can be applied to the groups  $\text{SL}_k(\mathbb{Z}/(p^i\mathbb{Z}))$  (this is a special case of a more general setup where  $\text{SL}$  is replaced by a Chavelley group.) It turns out that the profinite completion in this case is naturally isomorphic to  $\text{SL}_k(\mathbb{Z}_p)$ .

For a profinite group  $G$  the Haar measure can be easily described as a “limit” of counting measures. More precisely, for an open set  $U \subseteq G$  we have,

$$(9) \quad \mu(U) = \lim_i \frac{|\phi_i(U)|}{|G_i|}.$$

### 3. PRODUCT-FREE MEASURE

In this section, we will first introduce the main object of study in this paper:

**Definition 1.** Let  $G$  be a compact group with normalized Haar measure  $\mu$ . Define the product-free measure of  $G$  by

$$\text{pf}(G) = \sup\{\mu(A) : A \subseteq G \text{ is measurable, } A \cap A^2 = \emptyset\}.$$

First note that  $\text{pf}(G) \leq 1/2$ . This follows from the fact that if  $A \cap A^2 = \emptyset$  then for each  $x \in A$ , the sets  $A$  and  $xA$  are disjoint and have the same Haar measure. One can also easily see that  $\text{pf}(G) > 0$ . Let  $G$  be a compact group. It is known that the topology of  $G$  is given by a bi-invariant metric (see Corollary A4.19 in [10].) Let  $d_G$  be such a metric and  $D = \text{diam}(G)$  be the diameter of  $G$ . Let us also denote  $f(r) = \mu(B(x, r))$  (note that the bi-invariance of  $d_G$  implies that volume of the ball is independent of the center.) Then we have

**Proposition 1.**

$$\text{pf}(G) \geq f(D/3) > 0.$$

**Proof:** Choose  $y, z \in G$  such that  $d_G(y, z) = D$  and let  $x = z^{-1}y$ . We have,

$$d_G(x, x^2) = d_G(1, x) = d_G(z, zx) = d_G(z, y) = D.$$

Now a simple application of triangle inequality shows that if  $u, v \in B(x, D/3)$  then  $uv \in B(x^2, 2D/3)$  and hence  $uv \notin B(x, D/3)$ . This shows that  $B(x, D/3)$  is product-free.  $\square$

Note that our first theorem shows that the above inequality turns into an equality for the one-dimensional torus. We would also like to remark that one can give an alternative definition by replacing  $A \cap A^2 = \emptyset$  with  $\mu(A \cap A^2) = 0$ . However, this turns out to be equivalent:

**Proposition 2.** Suppose  $G$  is an infinite compact group with Haar measure  $\mu$ . Define

$$\text{pf}_0(G) = \sup\{\mu(A) : A \subseteq G \text{ is measurable, } \mu(A \cap A^2) = 0\}$$

Then  $\text{pf}_0(G) = \text{pf}(G)$ .

**Proof:** It is clear that  $\text{pf}(G) \leq \text{pf}_0(G)$ . To prove the inverse inequalities, let  $A$  be a measurable set with  $\mu(A \cap A^2) = 0$ . Then  $B = A - (A \cap A^2) \subseteq A$  has the same measure as  $A$  and  $B \cap B^2 \subseteq B \cap A^2 = \emptyset$ . This shows that  $\text{pf}(G) \leq \text{pf}_0(G)$ .  $\square$

It is possible to exactly compute the value  $\text{pf}(G)$  for connected abelian Lie groups  $G$ . Let  $\mathbb{T}^k$  denote the  $k$ -dimensional torus. Then,

**Theorem 7.** *For any  $k \geq 1$  we have  $\text{pf}(\mathbb{T}^k) = 1/3$ .*

**Proof:** The proof is similar to the proof given in [11] where only open sets  $A$  are considered. We will show that in fact there is no need to restrict to consider just the open sets. We will write this part of the proof, which is valid for any compact group, using the multiplicative notation. Suppose that  $A$  is a product-free subset with  $\mu(A) = 1/3 + \beta$  for some  $\beta > 0$ . First choose a compact set  $K \subseteq A$  with  $\mu(K) \geq 1/3 + \beta/2$ . Clearly  $K$  is product-free and since  $K$  is compact  $d(K, K^2) = \epsilon > 0$  where we use  $d$  as a shorthand for  $d_{\mathbb{T}^k}$ . Let  $U$  be the  $\delta$ -neighborhood of  $K$ , i.e. the set of points  $u \in \mathbb{T}^k$  such that  $d(u, k) < \delta$  for some  $k \in K$ . We will show that for  $\delta$  small enough  $U$  will be product-free as well. Let  $u_1, u_2, u_3 \in U$ . So there exist  $k_1, k_2, k_3 \in K$  such that  $d(u_i, k_i) < \delta$  for  $i = 1, 2, 3$ . Using the invariance of  $d$  we have

$$\begin{aligned} d(u_2 u_3, k_2 k_3) &\leq d(u_2 u_3, k_2 u_3) + d(k_2 u_3, k_2 k_3) \\ &= d(u_2, k_2) + d(u_3, k_3) < 2\delta \end{aligned}$$

From here we have  $d(u_1, u_2 u_3) \geq d(k_1, k_2 k_3) - d(k_1, u_1) - d(k_2 k_3, u_2 u_3) \geq \epsilon - 3\delta$ . So if we choose  $\delta = \epsilon/4$  we will have  $d(u_1, u_2 u_3) > \epsilon/4$  which shows that  $U \cap U^2 = \emptyset$ .

Now let us assume that  $A$  is an open product-free subset of  $\mathbb{T}^k = \mathbb{T}^1 \times \cdots \times \mathbb{T}^1$  with  $\mu(A) = 1/3 + \beta$ . Again, by possibly exchanging  $\beta$  with  $\beta/2$  we can assume that  $A$  is a union of boxes of the form:  $I_1 \times I_2 \cdots \times I_k$  where  $I_j$  is an interval in the  $j$ -th copy of  $\mathbb{T}^1$ . Choose a large prime number  $p$ . Set  $\zeta = \exp(2\pi i/p)$  and let  $G_p$  be the elementary abelian  $p$ -group in  $\mathbb{T}^k$  consisting of all elements of order  $p$ . Note that  $G$  contains  $p^k$  elements. Consider a box  $I_1 \times I_2 \cdots \times I_k$  and let  $h_j$  be the length of  $I_j$ . It is easy to see that

$$|G_p \cap I| \geq (ph_1 - 1) \cdots (ph_k - 1) = p^k \mu(I) + O(p^{k-1}).$$

By adding up over all boxes we will get

$$|G_p \cap A| \geq p^k \mu(A) + O(p^{k-1}).$$

Since  $G_p$  is a finite  $p$ -group, by Green-Ruzsa theorem (see Theorem 8) we have  $\text{pf}(G_p) \leq 1/3 + 1/(3p)$ . Since  $A$  is product free we must have

$$(1/3 + \beta/2) + O(1/p) \leq 1/3 + 1/(3p),$$

which as  $p \rightarrow \infty$  gives a contradiction.  $\square$

**Lemma 1.** *Let  $H$  be a proper subgroup of a finite group  $G$ . Then  $G$  contains a subset of density  $[G : H]^{-1}$  which is product-free. Similarly, if  $G$  is a profinite group and  $H$  is a proper open subgroup, then  $G$  contains an open product-free set of measure  $[G : H]^{-1}$ .*

**Proof:** Let  $A = xH$  be a left coset of  $H$  other than  $H$ . It is easy to see that  $A \cdot A \cap A = \emptyset$ .  $\square$

For finite abelian groups, the exact value of  $\text{pf}(G)$  is explicitly given by:

**Theorem 8.** (Green-Ruzsa, cf. [7]) Suppose  $G$  is a finite abelian group of size  $n$ .

- (1) If  $n$  is divisible by a prime  $p \equiv 2 \pmod{3}$ , then  $\text{pf}(G) = 1/3 + 1/(3p)$  where  $p$  is the smallest such  $p$ .
- (2) Otherwise, if  $3|n$ , then  $\text{pf}(G) = 1/3$ .
- (3) Otherwise,  $\text{pf}(G) = 1/3 - 1/(3m)$  where  $m$  is the largest order of any element of  $G$ .

Using Theorem 8 we will prove our first theorem.

**Proof of Theorem 1:** First we will give the proof for  $\mathbb{Z}_p$ . Let  $\phi_n : \mathbb{Z}_p \rightarrow \mathbb{Z}/(p^n\mathbb{Z})$  be reduction modulo  $p^n$  for  $n \geq 1$ . For  $p \equiv 2 \pmod{3}$ , it is easy to verify that if  $S \subseteq \mathbb{Z}/(p\mathbb{Z})$  is a product-free set of density  $1/3 + 1/(3p)$ , provided by Green-Ruzsa theorem, then  $\phi_1^{-1}(S) \subseteq \mathbb{Z}_p$  will be a set of the same density. For  $p \equiv 1 \pmod{3}$ , consider the subset of  $\mathbb{Z}/(p^n\mathbb{Z})$ :

$$S_n = \left\{ \left\lfloor \frac{p^n}{3} \right\rfloor + 1, \dots, \left\lfloor \frac{2p^n}{3} \right\rfloor \right\} + \mathbb{Z}/(p^n\mathbb{Z}).$$

By Lemma 1 we have

$$\text{pf}(\mathbb{Z}_p) \geq \sup_{n \geq 1} \frac{|S_n|}{p^n} = \sup_{n \geq 1} \frac{\left\lfloor \frac{2p^n}{3} \right\rfloor - \left\lfloor \frac{p^n}{3} \right\rfloor}{p^n} = \frac{1}{3}.$$

On the other hand, suppose  $A$  is a measurable product-free subset of  $\mathbb{Z}_p$  or  $\mathbb{F}_p[[t]]$  with  $\mu(A)$  larger than the function given on the right side of (1), that we denote it by  $f(p)$ . Choose a compact subset  $A_1 \subseteq A$  such that  $\mu(A_1) = f(p)(1 + \epsilon)$  for some  $\epsilon > 0$ . By the equation 9, this can be seen in a sufficiently finite quotient of  $\mathbb{Z}_p$ , i.e., for sufficiently large  $n$ , the set  $\phi_n(A_1) \subseteq \mathbb{Z}/(p^n\mathbb{Z})$  has a density larger than  $f(p)(1 + \epsilon/2)$ . By the theorem of Green and Ruzsa, this implies that there exist  $x_n, y_n, z_n \in A_1$  such that  $\phi_n(x_n y_n z_n^{-1}) = 1$ . Since  $A_1$  is compact, after passing to a subsequence, there exist  $x, y, z \in A_1$  such that  $x_n \rightarrow x, y_n \rightarrow y, z_n \rightarrow z$ . Now, since  $x_n y_n z_n^{-1} \rightarrow 1$ , we have  $xy = z$ , which is a contradiction.

The proof for  $\mathbb{F}_p[[t]]$  is similar. The only difference is that all of the finite quotients of  $\mathbb{F}_p[[t]]$  are elementary  $p$ -groups. Hence when  $p \equiv 1 \pmod{3}$ , it is the third condition in Green-Ruzsa theorem that applies.  $\square$

#### 4. COMPLEX REPRESENTATIONS OF PROFINITE GROUPS

In this section we will gather some facts about profinite groups that will be used later. Our final aim in this section is to show that any non-trivial complex continuous representation of  $\text{SL}_k(\mathbb{Z}_p)$  factors through a non-trivial representation of  $\text{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$  for some  $n$ . In the next section we will find a lower bound for such a representations.

A topological group which is the projective limit of finite groups, each equipped the discrete topology, is called a profinite group. Such a group is compact and totally disconnected. We call a family  $\mathcal{I}$  of normal subgroups of an arbitrary group  $G$  a filter base if for all  $K_1, K_2 \in \mathcal{I}$  there is a subgroup  $K_3 \in \mathcal{I}$  which is contained in  $K_1 \cap K_2$ . Now let  $G$  be a topological group and  $\mathcal{I}$  a filter base of closed normal subgroups, and for  $K, L \in \mathcal{I}$  define  $K \leq' L$  if and only if  $L$  is a subgroup of  $K$ . Thus  $\mathcal{I}$  is a directed set with respect to the order  $\leq'$  and the surjective homomorphisms  $q_{KL} : G/L \rightarrow G/K$ , defined for  $K \leq' L$ , make the groups  $G/K$  into an inverse system. Write

$$\widehat{G} = \varprojlim (G/K).$$



There is a continuous homomorphism

$$\theta : G \longrightarrow \widehat{G}$$

with kernel  $\bigcap_{K \in \mathcal{I}} K$ , whose image is dense in  $\widehat{G}$ . We have the following

**Proposition 3** (See [17], proposition 1.2.2). *If  $G$  is compact then  $\theta$  is surjective; if  $G$  is compact and  $\bigcap_{K \in \mathcal{I}} K = \{id\}$  then  $\theta$  is an isomorphism of topological groups.*

Moreover we have,

**Proposition 4** (See [17], proposition 1.2.1). *Let  $(G, \varphi_n)$  be an inverse limit of an inverse system  $(G_n)$  of compact Hausdorff topological groups and let  $L$  be an open normal subgroup of  $G$ . Then  $\ker \varphi_n \leq L$  for some  $n$ .*

For the profinite group  $\mathrm{SL}_k(\mathbb{Z}_p)$  let consider the following surjective homomorphism

$$0 \longrightarrow K_n \longrightarrow \mathrm{SL}_k(\mathbb{Z}_p) \xrightarrow{\varphi_n} \mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z})) \longrightarrow 0,$$

where  $\varphi_n$  is induced by the canonical surjective homomorphism  $\mathbb{Z}_p \longrightarrow \mathbb{Z}/(p^n\mathbb{Z})$ . Clearly the set  $\mathcal{I}$  consists of  $K_n$  is a filter base and  $\bigcap K_n = I$ , therefore by Proposition 3 we have

$$\mathrm{SL}_k(\mathbb{Z}_p) = \varprojlim \mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z})).$$

The following proposition is a standard fact in the context of the Galois representation, however for the sake of completeness we will prove it.

**Proposition 5.** *Let  $G$  be a profinite group, and assume  $\rho : G \longrightarrow \mathrm{GL}_m(\mathbb{C})$  is a continuous representation. Then the kernel of  $\rho$  is an open subgroup, hence  $\mathrm{Im}(\rho)$  is a finite subgroup of  $\mathrm{GL}_m(\mathbb{C})$ .*

**Proof:** First we show that there exists a neighborhood of the identity element in  $\mathrm{GL}_m(\mathbb{C})$  that does not contain any subgroup other than the trivial subgroup. Let  $\exp : \mathfrak{gl}_m(\mathbb{C}) \longrightarrow \mathrm{GL}_m(\mathbb{C})$  be the exponential map of the Lie group  $\mathrm{GL}_m(\mathbb{C})$  and  $U_1$  an open neighborhood of  $0 \in \mathfrak{gl}_m(\mathbb{C})$  on which  $\exp$  is a diffeomorphism. Set  $U = (1/2)U_1$  (If it is necessarily we will take  $(1/2^k)U_1$  for some  $k$  big enough). Let  $H$  be a non-trivial subgroup of  $\mathrm{GL}_m(\mathbb{C})$  contained in  $\exp(U)$ . Then one can choose  $X \in U$  such that  $a = \exp(X) \in H$  and  $2X \in U_1 \setminus U$ . This shows that  $a^2 = \exp(2X) \in \exp(U_1) \setminus \exp(U)$  which is a contradiction. Therefore  $U$  is a neighborhood of the identity element in  $\mathrm{GL}_m(\mathbb{C})$  that does not contain any subgroup other than the trivial subgroup.

Then  $V := \rho^{-1}(U)$  is an open subset of  $G$  containing the identity and from the properties of profinite groups, we know that  $V$  contains an open subgroup, say  $H$ . This implies that  $\rho(H) = 1$  and hence  $H \leq \ker \rho$ . Therefore  $\ker \rho$  is open thus  $\mathrm{Im}(\rho)$  is finite.  $\square$

This can now imply the following:

**Theorem 9.** *Let  $\rho : \mathrm{SL}_k(\mathbb{Z}_p) \longrightarrow \mathrm{GL}_m(\mathbb{C})$  be a continuous non-trivial representation. Then  $\rho$  factors through a non-trivial representation of  $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$  for some  $n$ .*

**Proof:** By Proposition 5,  $\ker \rho$  is an open normal subgroup, therefore by Proposition 4, for some  $n$ ,  $K_n \leq \ker \rho$ , where

$$0 \longrightarrow K_n \longrightarrow \mathrm{SL}_k(\mathbb{Z}_p) \xrightarrow{\varphi_n} \mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z})) \longrightarrow 0.$$

Therefore  $\rho$  factors through to a non-trivial representation of

$$\bar{\rho} : \mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z})) \longrightarrow \mathrm{GL}_m(\mathbb{C}).$$

$\square$



## 5. REPRESENTATIONS OF FINITE QUOTIENTS

In this section we will give a bound on the dimension of non-trivial complex continuous representation of  $\mathrm{SL}_k(\mathbb{Z}_p)$  where  $\mathbb{Z}_p$  stands for the ring of  $p$ -adic integers. The first result regarding to this type of bound goes back to Frobenius who proved that the dimension of any non-trivial representation of  $\mathrm{PSL}_2(\mathbb{F}_p)$  is at least  $(p-1)/2$ . Also he proved that this bound is sharp.

**Definition 2.** For  $G := \mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$ , where  $p$  is an odd prime, define  $m(p, k, n)$  to be the smallest  $t$  such that  $G$  has a non-trivial representation of degree  $t$ .

Our main theorems in this section are the following

**Theorem 10.** Let  $p$  be an odd prime number. For  $G := \mathrm{SL}_2(\mathbb{Z}/(p^n\mathbb{Z}))$

$$m(p, 2, n) \geq \frac{p-1}{2}.$$

For  $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$  for  $k \geq 3$  we have a similar theorem:

**Theorem 11.**

$$m(p, k, n) \geq p^{k-1} - p^{k-2}.$$

**Proof of Theorem 4:** Using Theorems 10 and 11 along with Theorem 9, we can establish Theorem 4.  $\square$

**Proof of Theorem 10:** Let  $\rho : \mathrm{SL}_2(\mathbb{Z}/(p^n\mathbb{Z})) \rightarrow \mathrm{GL}_d(\mathbb{C})$  be a non-trivial representation of the group  $\mathrm{SL}_2(\mathbb{Z}/(p^n\mathbb{Z}))$  with  $d < \frac{p-1}{2}$ . Set

$$a := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Let  $A := \rho(a) \neq I$ . Since the order of  $a$  is  $p^n$ , therefore  $A$  has a non-trivial eigenvalue, say  $\zeta$ , which is a  $p^n$ -th root of unity. Notice that  $a$  is conjugate to  $a^m$ , where  $m$  is a square in  $\mathbb{Z}/(p^n\mathbb{Z})$ . Hereafter  $m$  will be an arbitrary quadratic residue in  $\mathbb{Z}/(p^n\mathbb{Z})$ . This implies that  $A$  and  $A^m$  would have the same set of eigenvalues. But  $\zeta^m$  are the eigenvalues of  $A^m$ . Notice that there are at least  $\frac{p-1}{2}$  different value of  $\zeta^m$  and hence  $d \geq \frac{p-1}{2}$  which is a contradiction. This implies that  $\rho(a) = I$ . The same argument for

$$b := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

shows that  $\rho(b) = I$ . But  $\mathrm{SL}_2(\mathbb{Z}/(p^n\mathbb{Z})) = \langle a, b \rangle$ , which implies that  $\rho$  is the trivial representation.  $\square$

Now let us show that for  $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$  the minimum dimension of non-trivial representation is at least  $p^{k-1} - p^{k-2}$ . Let

$$\rho : \mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z})) \rightarrow \mathrm{GL}_d(\mathbb{C}),$$

be a non-trivial representation of  $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$ . Let  $H$  be the subgroup of  $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$  consisting of matrices of the form

$$H = \left\{ k(M) = \begin{pmatrix} M_{(k-1) \times (k-1)} & 0_{(k-1) \times 1} \\ 0_{1 \times (k-1)} & 1 \end{pmatrix} : M_{(k-1) \times (k-1)} \in \mathrm{SL}_{k-1}(\mathbb{Z}/(p^n\mathbb{Z})) \right\}.$$

Let  $L$  be the subgroup of  $\mathrm{SL}_k(\mathbb{Z}/(p^n\mathbb{Z}))$  defined by

$$L = \left\{ l(w) = \begin{pmatrix} I_{(k-1) \times (k-1)} & w_{(k-1) \times 1} \\ 0_{1 \times (k-1)} & 1 \end{pmatrix} : w_{(k-1) \times 1} \in (\mathbb{Z}/(p^n\mathbb{Z}))^{k-1} \right\}.$$

It is easy to see that  $H$  normalizes  $L$  and the action by conjugation of  $H$  on  $L$  is given by

$$(10) \quad k(M)l(w)k(M)^{-1} = l(Mw).$$

Let  $a = E_{1n} \in L$  denotes the elementary matrix such the only non-zero entry of  $E_{1n} - I$  is the  $(1, n)$ -th entry, which is 1. Note that if  $\rho(a) = I$  then  $\rho$  is a trivial representation. Indeed  $\mathrm{SL}(\mathbb{Z}/(p^n\mathbb{Z}))$  is generated by elementary matrices, and all elementary matrices are conjugate to  $a$ .

**Definition 3.** Let  $\mathcal{S}$  be a family of matrices in  $M_n(\mathbb{C})$ . For a function  $r : \mathcal{S} \rightarrow \mathbb{C}$  define

$$V(r) = \{v \in \mathbb{C}^n : Sv = r(S)v \text{ for all } S \in \mathcal{S}\}.$$

A map  $r : \mathcal{S} \rightarrow \mathbb{C}$  will be called a root of  $\mathcal{S}$  if  $V(r) \neq \{0\}$ . Moreover  $V(r)$  is called a root subspace.

The following proposition is a special case of Theorem 15 in section 9.5. of [9].

**Proposition 6.** Let  $\mathcal{S}$  be a commuting family of  $d \times d$  unitary matrices. Then  $\mathcal{S}$  has only a finite number of roots. If  $r_1, \dots, r_t$  are all the distinct roots of  $\mathcal{S}$  then

- (1)  $V(r_i)$  is orthogonal to  $V(r_j)$  for  $i \neq j$ .
- (2)  $\mathbb{C}^d = V(r_1) \oplus \dots \oplus V(r_t)$ .

Note that  $\mathcal{S} = \rho(L)$  is an abelian group and  $H$  acts on the root functions and root subspaces of  $\mathcal{S}$ .

**Proposition 7.** Let  $r$  be one of the roots in the decomposition in Proposition 6 and  $h \in H$ . Then for any  $s \in \mathcal{S}$ , let  $s = \rho(l)$ , then

$$r_h(s) := r(\rho(hlh^{-1}))$$

is also a root for  $\mathcal{S}$ , and  $V(r_h) = \rho(h^{-1})V(r)$ .

**Proof:** First note that since  $H$  normalizes  $L$ , the map  $r_h$  is well-defined. For  $w \in V(r), l \in L$ , we have

$$\rho(l)(\rho(h^{-1})w) = \rho(h^{-1})(\rho(hlh^{-1})w) = r(\rho(hlh^{-1}))\rho(h^{-1})w = r_h(\rho(l))(\rho(h^{-1})w).$$

This shows that  $r_h$  is a root for  $\mathcal{S}$ , and  $\rho(h^{-1})V(r) \subseteq V(r_h)$ . To show the equality let  $v \in V(r_h)$ , then for any  $l \in L$  we have

$$\rho(l)(\rho(h)v) = \rho(h)(\rho(h^{-1}lh)v) = r(\rho(l))(\rho(h)v),$$

so  $\rho(h)V(r_h) \subseteq V(r)$ . □

Now we can prove Theorem 11.

**Proof of Theorem 11:** First note that  $L$  as an abstract group is isomorphic to the direct sum of  $k - 1$  copies of the cyclic group  $\mathbb{Z}/(p^n\mathbb{Z})$ . Let  $e_1, \dots, e_{k-1}$  be the standard basis for  $L$ : each  $e_i$  has all entries equal to zero, except the entry at the  $i$ -th row which is equal to one. We will occasionally deviate from our standard notation for the group operation and use additive notation for group operation on  $L$ , when this isomorphism is used. For instance, we will write  $e_1 + e_2$  instead of  $e_1 \cdot e_2$ .

One of the consequences of the above discussion is that every  $l \in L$  we have  $\rho(l)^{p^n} = I$ , and hence all of the eigenvalues of  $\rho(l)$  are  $p^n$ -th roots of unity. Set  $\zeta = \exp(2\pi i/p^n)$ . Let  $r$  be one of the roots which is different from 1. Such a root exists since  $\rho$  is not the trivial representation. This shows that  $r(\rho(e_i)) \neq 1$  for some  $1 \leq i \leq k-1$ . Without loss of generality assume that  $i = 1$  and  $r(\rho(e_1)) = \zeta^{m_1}$  with  $1 \leq m_1 \leq p^n - 1$ . We also assume that for  $2 \leq i \leq k-1$  we have  $r(\rho(e_i)) = \zeta^{m_i}$  where  $0 \leq m_i \leq p^n - 1$ . For  $t \in (\mathbb{Z}/(p^n\mathbb{Z}))^*$  and  $x_2, \dots, x_{k-1} \in \mathbb{Z}/(p^n\mathbb{Z})$  whose values will later be assigned, define

$$k_1 = k(t, x_2, \dots, x_{k-1}) = \begin{pmatrix} t & x_2 & \cdots & x_{k-1} & 0 \\ 0 & t^{-1} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \in H$$

Using 10, a simple computation shows that

$$k_1 e_1 k_1^{-1} = t e_1, \quad k_1 e_2 k_1^{-1} = t^{-1} e_2 + x_2 e_1, \quad k_1 e_i k_1^{-1} = e_i + x_i e_1, \quad 3 \leq i \leq k-1.$$

By Proposition 7, we have  $r_{t, x_2, \dots, x_{k-1}} := r_{k_1}$  is a root and

$$\begin{aligned} r_{t, x_2, \dots, x_{k-1}}(\rho(e_1)) &= r(\rho(k_1 e_1 k_1^{-1})) = r(\rho(t e_1)) = \zeta^{t m_1}. \\ r_{t, x_2, \dots, x_{k-1}}(\rho(e_2)) &= r(\rho(k_1 e_2 k_1^{-1})) = r(\rho(t^{-1} e_2 + x_2 e_1)) = \zeta^{t^{-1} m_2 + x_2 m_1}, \\ r_{t, x_2, \dots, x_{k-1}}(\rho(e_i)) &= r(\rho(k_1 e_i k_1^{-1})) = r(\rho(e_i + x_i e_1)) = \zeta^{m_i + x_i m_1}, \end{aligned}$$

for  $3 \leq i \leq k-1$ . Now, since  $m_1$  has order at least  $p$ , by varying the values of  $t, x_2, \dots, x_{k-1}$  we can get at least  $(p-1)p^{k-2} = p^{k-1} - p^{k-2}$  different roots. This shows that the dimension of the representation space has to be at least  $p^{k-1} - p^{k-2}$ .  $\square$

## 6. HILBERT-SCHMIDT OPERATORS AND PRODUCT-FREE SETS IN COMPACTS GROUPS

This section includes some other ingredients of the proof from functional analysis. We are not trying to give a complete proof of these facts. The reader can consult with [15] for details. After reviewing these facts we will give a proof for Theorem 2 and Corollary 1. Let  $G$  be a compact, second countable, Hausdorff topological group with a normalized Haar measure  $\mu$ . As usual, define,

$$L^2(G) := \left\{ h : G \longrightarrow \mathbb{C} : \int_G |h|^2 d\mu < \infty \right\}.$$

Notice that  $L^2(G)$  with the following norm is a separable Hilbert space.

$$\|h\|_2^2 := \int_G |h|^2 d\mu.$$

Moreover, let us define  $L_0^2(G)$  to be the set of all functions in  $L^2(G)$  which are orthogonal to the constant function 1:

$$L_0^2(G) := \left\{ h \in L^2(G) : \int_G h d\mu = 0 \right\}.$$

For  $f_1, f_2 \in L^2(G)$ , the convolution  $f_1 * f_2 \in L^2(G)$  is defined by

$$(f_1 * f_2)(x) := \int_G f_1(xy^{-1})f_2(y) d\mu(y).$$

For any given  $f_1, f_2 \in L^2(G)$ , from the Cauchy-Schwartz inequality we have

$$(11) \quad \|f_1 * f_2\|_2 \leq \|f_1\|_2 \|f_2\|_2.$$

Our objective in this section is to prove a stronger form of this inequality. For finite groups, Gowers [6] applies the singular value decomposition to the adjacency matrix attached to a finite bipartite graph, to obtain a stronger inequality. In order to generalize this to all compact groups, we will invoke Hilbert-Schmidt integral operator along with the singular value decomposition (compare this to inequality (11)). Assume  $f_1 \in L_0^2(G)$ . To prove Theorem 2 note that by subtracting the constant  $c = \int_G f_1 d\mu$  from  $f_2$  and noticing that  $f_1 * c = 0$ , without loss of generality, we can assume that  $f_2 \in L_0^2(G)$ . We consider the following kernel

$$K(x, y) := f_1(xy^{-1}).$$

Since  $G$  is a compact group, then we have  $K(x, y) \in L^2(G \times G)$ . For this kernel, we define the following integral operator

$$(12) \quad \begin{aligned} \Phi_K : L_0^2(G) &\longrightarrow L_0^2(G) \\ h &\longmapsto \Phi_K(h), \end{aligned}$$

where

$$(13) \quad \Phi_K(h)(x) := \int_G K(x, y)h(y)d\mu(y) \in L_0^2(G).$$

It is clear that  $\Phi_K(h)(x) = (f_1 * h)(x)$ . In order to prove Theorem 2, we need to show that

$$(14) \quad \|\Phi_K\|_{L_0^2(G)}^2 \leq \frac{1}{\ell} \|f_1\|_2^2.$$

One can easily see that

$$\Phi_K^*(h)(y) = \int_G \overline{K(y, x)}h(x)d\mu(x).$$

Since  $G$  is not commutative,  $\Phi_K$  is not necessarily a self adjoint operator. We will show that  $\Phi_K$  is a compact operator.

**Definition 4.** Let  $\mathcal{H}$  be a separable Hilbert space with an orthonormal basis  $\{e_n\}$  and let  $T \in B(\mathcal{H})$ , where  $B(\mathcal{H})$  denotes the set of bounded operator. If the condition

$$\sum_{n=1}^{\infty} \|T(e_n)\|^2 < \infty,$$

holds then  $T$  is called a Hilbert-Schmidt operator.

This condition does not depend on the choice of the orthonormal basis of  $\mathcal{H}$ . In fact, for a Hilbert-Schmidt operator  $T$ , the value of the sum is independent of the choice of the orthonormal basis:

$$\|T\|_{HS}^2 := \sum_{n=1}^{\infty} \|T(e_n)\|^2.$$

We have the following properties of Hilbert-Schmidt operators.

**Lemma 2.** *Let  $\mathcal{H}$  be a separable Hilbert space and let  $T \in B(\mathcal{H})$  then*

- a)  *$T$  is Hilbert-Schmidt if and only if  $T^*$  is Hilbert-Schmidt.*
- b) *If either  $S$  or  $T$  is Hilbert-Schmidt, then  $ST$  is Hilbert-Schmidt.*
- c) *If  $T$  is Hilbert-Schmidt then it is compact.*

Over  $L^2(G)$  we have a characterization of Hilbert-Schmidt operators. Indeed, for  $K \in L^2(G \times G)$ , consider the operator  $\Phi_K$ , as it defined in (13), which is called an integral operator with the kernel  $K$ . We have,

**Lemma 3.** *The integral operator  $\Phi_K : L^2(G) \longrightarrow L^2(G)$  is a Hilbert-Schmidt operator and hence is compact. The norm of  $\Phi_K$  is given by,*

$$(15) \quad \|\Phi_K\|_{HS} = \|K\|_{L^2(G \times G)}.$$

And the last ingredient in order to prove Theorem 2 is the following lemma.

**Lemma 4** (singular value decomposition). *Let  $\mathcal{H}$  be a separable Hilbert space and  $T \in B(\mathcal{H})$  be a compact operator. Then there exists two orthonormal sets  $\{e_n\}$  and  $\{e'_n\}$  in  $\mathcal{H}$  such that*

$$T(e_i) = \lambda_i e'_i, \quad T^*(e'_i) = \lambda_i e_i, \quad i = 1, 2, \dots$$

where

$$\lambda_1 \geq \lambda_2 \geq \dots \geq 0,$$

and for any  $x \in \mathcal{H}$

$$(16) \quad T(x) = \sum_{i \geq 1} \lambda_i \langle x, e_i \rangle e'_i.$$

Moreover, by (16), we have  $\|T\| = \lambda_1$ .

Using these lemmas we will now prove:

**Proof of Theorem 2:** Consider the operator

$$\Phi_K : L_0^2(G) \longrightarrow L_0^2(G),$$

defined by equation (12) and apply the singular value decomposition to obtain orthonormal bases  $\{e_n\}$  and  $\{e'_n\}$  in  $L_0^2(G)$  such that

$$\Phi_K(e_i) = \lambda_i e'_i,$$

where

$$\lambda_1 \geq \lambda_2 \geq \dots \geq 0.$$

Moreover  $\|\Phi_K\|_{L^2_0(G)} = \lambda_1$ . For  $\Phi_K^* \Phi_K$ , which is a self-adjoint Hilbert-Schmidt operator, let  $V_1$  be the eigenspace of  $\Phi_K^* \Phi_K$  correspondence to  $\lambda_1^2$ . Since  $\Phi_K^* \Phi_K$  is a compact operator then  $\dim V_1 < \infty$ . We have

$$\begin{aligned} \|\Phi_K\|^2 \dim V_1 &= \lambda_1^2 \dim(V_1) \leq \sum_{i=1}^{\infty} \lambda_i^2 = \|\Phi_K^* \Phi_K\|_{HS}^2 \\ &\leq \|\Phi_K\|_{HS}^2 = \|K\|_{L^2(G \times G)}^2 \\ &= \int_G \int_G |f_1(xy^{-1})|^2 d\mu(y) d\mu(x) = \|f_1\|_2^2. \end{aligned}$$

We show that  $\dim V_1 \geq \ell$ , and this would finish the proof. We will construct an action of  $G$  on  $V_1$  by defining for every  $h \in V_1$  and  $g \in G$

$$T_g h(x) := h(xg).$$

We need to verify that,

$$(17) \quad T_g(\Phi_K^* \Phi_K(h)) = \Phi_K^* \Phi_K(T_g h).$$

Since  $G$  is compact and hence unimodular we have,

$$\begin{aligned} \Phi_K(T_g h)(x) &= \int_G f_1(xy^{-1}) h(yg) d\mu(y) \\ &= \int_G f_1(x(zg^{-1})^{-1}) h(z) d\mu(z) \\ &= \int_G f_1(xgz^{-1}) h(z) d\mu(z) \\ &= T_g(\Phi_K(h))(x). \end{aligned}$$

By acting  $\Phi_K^*$  from the left we obtain 17. Since  $V_1$  is a subspace of  $L^2_0(G)$ , it does not contain the constant function, and hence this linear action is non-trivial. This induces a non-trivial representation of  $G$  in the unitary group  $U(V_1)$ , thus  $\dim V_1 \geq \ell$ .  $\square$

**Proof of Corollary 1.** Apply the inequality to  $f_1 = 1_A$  and  $f_2 = 1_B - \mu(B)$ .  $\square$

## 7. PROOF OF THE MAIN THEOREMS

This section is devoted to the proof of Theorems 3, and Theorem 5.

**Proof of Theorem 3:** The proof is very similar to the proof of an analogous theorem for finite groups obtained by Gowers [6]. Let

$$S = \{y \in G : (1_A * 1_B)(y) = 0\}.$$

Thus

$$\begin{aligned}\mu(S)^{1/2}\mu(A)\mu(B) &= \left( \int_S |(1_A * 1_B)(y) - \mu(A)\mu(B)|^2 d\mu(y) \right)^{1/2} \\ &\leq \left( \int_G |(1_A * 1_B)(y) - \mu(A)\mu(B)|^2 d\mu(y) \right)^{1/2} \\ &= \|1_A * 1_B - \mu(A)\mu(B)\|_2.\end{aligned}$$

But via Corollary 1 we can deduce that

$$\mu(S)^{1/2}\mu(A)\mu(B) \leq \sqrt{\frac{\mu(A)\mu(B)}{\ell}},$$

therefore

$$\mu(S) \leq \frac{1}{\ell\mu(A)\mu(B)}.$$

This implies that  $C \not\subseteq S$ , since otherwise we get

$$\mu(C)\mu(A)\mu(B) \leq \frac{1}{\ell},$$

which is a contradiction. Hence there exists  $y \in C$  so that  $1_A * 1_B(y) \neq 0$ , which means that  $AB \cap C \neq \emptyset$ .

For the second statement let define

$$\Sigma := \{(a, b, c) \in A \times B \times C : ab = c\}.$$

Notice that

$$(18) \quad \mu(\Sigma) = \langle 1_A * 1_B, 1_C \rangle = \langle 1_A * (1_B - \mu(B)), 1_C \rangle + \mu(A)\mu(B)\mu(C).$$

By Cauchy-Schwartz inequality we have

$$\begin{aligned}\langle 1_A * (1_B - \mu(B)), 1_C \rangle^2 &\leq \|1_A * (1_B - \mu(B))\|_2^2 \|1_C\|_2^2 \\ &= \|1_A * 1_B - \mu(A)\mu(B)\|_2^2 \mu(C) \\ &\leq \frac{\mu(A)\mu(B)\mu(C)}{\ell}.\end{aligned}$$

Thus if

$$\frac{\mu(A)\mu(B)\mu(C)}{\ell} \leq \eta^2 \mu(A)^2 \mu(B)^2 \mu(C)^2,$$

which is fulfilled by our assumption, we deduce that

$$|\langle 1_A * (1_B - \mu(B)), 1_C \rangle| \leq \eta \mu(A)\mu(B)\mu(C),$$

thus

$$\mu(\Sigma) \geq \mu(A)\mu(B)\mu(C) - \eta \mu(A)\mu(B)\mu(C) = (1 - \eta)\mu(A)\mu(B)\mu(C)$$

□



**Remark 3.** One can also establish another inequality. For  $f_1 = 1_A$  and  $f_2 = 1_B - \mu(B)$ , notice that

$$\|f_2\|_2^2 = \mu(B)(1 - \mu(B)).$$

Thus by Theorem 2 we have

$$\mu(G - AB)^{1/2} \mu(A) \mu(B) \leq \sqrt{\frac{1}{\ell}} \mu(A)^{1/2} (\mu(B)(1 - \mu(B)))^{1/2},$$

therefore

$$1 - \frac{1 - \mu(B)}{\ell \mu(A) \mu(B)} \leq \mu(AB).$$

Now we can prove the main theorems of our paper.

**Proof of Theorem 5:** By Theorem 3 we observe that if for a measurable subset  $A \subseteq G$ ,

$$\mu(A) > \frac{1}{\ell^{1/3}},$$

then  $A^2 \cap A \neq \emptyset$ , where  $\ell$  is the minimal dimension of all non-trivial continuous representation of  $G$ . For  $G = \mathrm{SL}_k(\mathbb{Z}_p)$ , by Theorem 4 we have

$$\begin{aligned} \ell &\geq p^{k-1} - p^{k-2} \quad \text{for } k \geq 3, \\ \ell &\geq \frac{p-1}{2} \quad \text{for } k = 2. \end{aligned}$$

This will give the upper bound.

Therefore we only need to prove the lower bounds. Consider the reduction map

$$\phi : \mathrm{SL}_k(\mathbb{Z}_p) \longrightarrow \mathrm{SL}_k(\mathbb{Z}/(p\mathbb{Z})),$$

and let  $Q$  be the subgroup consisting of all matrices  $g \in \mathrm{SL}_k(\mathbb{Z}/(p\mathbb{Z}))$  such that

$$g_{1k} = \cdots = g_{k-1,k} = 0.$$

A simple counting shows that:

$$[\mathrm{SL}_k(\mathbb{Z}/(p\mathbb{Z})) : Q] = \frac{p^k - 1}{p - 1}.$$

Applying Lemma 1 establishes the lower bound. □

## 8. AUTOMORPHISMS OF THE REGULAR TREE

Let  $T_{k+1}$  be a regular tree of degree  $k+1$ . By an automorphism of  $T_{k+1}$  we mean a permutation of the set of vertices of  $T_{k+1}$  that preserves adjacency. The group of (simplicial) automorphisms of  $T_{k+1}$  with the topology of pointwise convergence is a locally compact group. We denote this group by  $\mathrm{Aut}$ . Note that  $\mathrm{Aut}(T_{k+1})$  acts transitively on  $T_{k+1}$ . Let  $O$  be one of the vertices of  $T_{k+1}$  to which we may occasionally refer as the root. For vertices  $v$  and  $w$  of  $T_{k+1}$ , let  $d(v, w)$  denote the distance between vertices  $v$  and  $w$ , i.e. the length of the shortest path joining  $v$  and  $w$ . Let  $A_{k+1}$  be the stabilizer of  $O$  in  $\mathrm{Aut}(T_{k+1})$ . It is easy to see that  $A_{k+1}$  is a profinite group. In fact, every  $x \in A_{k+1}$  fixes  $O$  and thereby permutes the set of all  $(k+1)k^{d-1}$  vertices of distance  $d$  from  $O$ , for every  $d \geq 1$ . This induces a homomorphism  $\sigma_d : A_{k+1} \longrightarrow \Sigma_{(k+1)k^{d-1}}$  where  $\Sigma_m$  denotes the

symmetric group on  $\{1, 2, \dots, m\}$ . We can now define the following “congruence subgroups” that provide a system of fundamental open sets around the identity automorphism:

$$C_d = \{x \in A_{k+1} : \sigma_j(x) = id, j \leq d\}$$

For more details we refer the reader to [3].

**Definition 5.** An automorphism  $x \in A_{k+1}$  is called *positive* if  $\sigma_d(x)$  is an even permutation for all  $d \geq 1$ . The group of all positive automorphisms is denoted by  $A_{k+1}^+$ .

In what follows let  $\text{Alt}_{k+1} \leq \Sigma_{k+1}$  denote the alternating group on  $k+1$  symbols. Note that  $\text{Alt}_k \leq \text{Alt}_{k+1}$  is a subgroup of index  $k+1$ . We will need the following fact from the representation theory of finite groups:

**Theorem 12** (See [5] Exercise 5.5). For  $n \geq 6$ , the minimum dimension of non-trivial representations of  $\text{Alt}_n$  is  $n-1$ .

**Proof of Theorem 6:** For the lower bound, note that  $\sigma_1 : A_{k+1}^+ \rightarrow \text{Alt}_{k+1}$  is surjective. Let  $H = \sigma_1^{-1}(\text{Alt}_k)$  and apply Lemma 1 to obtain an open subgroup of index  $k+1$  in  $A_{k+1}^+$ . This establishes the lower bound.

For the upper bound, we need to show that an arbitrary finite quotients of  $A_{k+1}^+$  does not have any non-trivial representation of dimension less than  $k-1-\epsilon$ , where  $\epsilon = 0$  if  $k$  is even and  $\epsilon = 1$  when  $k$  is odd.

Let  $F = A_{k+1}^+/N$  be such a finite quotient. Since  $N$  contains  $C_d$  for some  $d \geq 1$ ,  $G/N$  will be a factor of  $G/C_j$  for some  $j \geq 1$ . So, without loss of generality, we can assume that  $N = C_j$  and  $F_j = A_{k+1}^+/C_j$ . We will show that this group does not have any non-trivial representation of dimension less than  $k-1-\epsilon$ . Suppose  $\rho$  be such a representation. For  $j = 1$ , we will get  $F_1 = \text{Alt}_{k+1}$  and there is nothing to prove. For  $j = 2$ , the quotient is isomorphic to

$$F_2 = \text{Alt}_{k+1} \ltimes \underbrace{(\Sigma_k \times \Sigma_k \times \dots \times \Sigma_k)}_{k+1}^+,$$

where the alternating group acts by permuting the factors and  $(\sigma_1, \dots, \sigma_{k+1}) \in (\Sigma_k \times \dots \times \Sigma_k)^+$  if and only if  $\prod_{i=1}^{k+1} \text{sgn}(\sigma_i) = 1$ .

If the restriction of  $\rho$  to  $\text{Alt}_{k+1}$  is non-trivial then we are done. Suppose that the restriction of  $\rho$  to  $\text{Alt}_{k+1}$  is trivial. Clearly

$$\text{Alt}_k \times \dots \times \text{Alt}_k \subseteq (\Sigma_k \times \dots \times \Sigma_k)^+.$$

Again, we can assume that the restriction of  $\rho$  to each one of the factors is trivial, since otherwise we can apply Theorem 12. So  $\rho$  factors through the quotient  $(\Sigma_k \times \dots \times \Sigma_k)^+ / (\text{Alt}_k \times \dots \times \text{Alt}_k)$ . Note that since the restriction of  $\rho$  to  $\text{Alt}_{k+1}$  is trivial we have

$$\rho(\sigma_1, \dots, \sigma_k, \sigma_{k+1}) = \rho(\sigma_{i_1}, \dots, \sigma_{i_k}, \sigma_{i_{k+1}}).$$

for any even permutation  $(i_1, \dots, i_k, i_{k+1})$  of the set  $\{1, \dots, k, k+1\}$ . So,  $\rho$  will be identity if we can show:

**Lemma 5.** Let  $k \geq 5$  be an integers and

$$L = \{(v_1, \dots, v_{k+1}) \in (\mathbb{Z}/(2\mathbb{Z}))^{k+1} : v_1 + \dots + v_{k+1} = 0\}.$$

Let  $\rho : L \rightarrow \mathrm{GL}_d(\mathbb{C})$  be a non-trivial representation of  $L$  such that  $\rho(v_1, \dots, v_{k+1}) = \rho(v_{i_1}, \dots, v_{i_{k+1}})$  for every even permutation  $(i_1, \dots, i_{k+1})$  of the set  $\{1, \dots, k+1\}$ . Then  $d \geq k - \epsilon$  where  $\epsilon = 0$  if  $k$  is even and  $\epsilon = 1$  when  $k$  is odd.

*Proof.* Let  $M = \ker \rho$  and suppose that  $M \neq 0$ . We will show that for odd  $k+1$  if  $|M| > 1$  and for even  $k+1$  if  $|M| > 2$  then  $M = L$ . Let  $0 \neq v = (v_1, \dots, v_{k+1}) \in M$  and let

$$I(v) = \{1 \leq i \leq k+1 : v_i = 1\}.$$

It is enough to show that there exists  $v \in M$  with  $|I(v)| = 2$ . For then  $M$  will contain every  $v$  with  $|I(v)| = 2$  which shows that  $M = L$ . Suppose  $0 \neq v \in M$  is chosen such that  $|I(v)|$  is minimal. Let  $|I(v)| = 2j > 2$  and without loss of generality assume that  $v = (1, 1, \dots, 1, 0, \dots, 0)$  where the first  $2j$  entries are equal to 1 and the rest are zero. If  $k+1$  is odd then we can consider the 3-cycle  $\sigma = (1, 2, 2j+1) \in \mathrm{Alt}_{k+1}$ . Now it is easy to see that  $\sigma \cdot v - v$  has 1 in only two positions which is a contradiction. The same can be done if  $k+1$  is even and  $|M| > 2$ . This implies that  $M = \{0\}$  and  $\rho$  is faithful, when  $k+1$  is odd and  $|M| \leq 2$  when  $k+1$  is even. In either case  $\rho(L)$  is isomorphic to the direct product of at least  $k - \epsilon$  copies of  $\mathbb{Z}/(2\mathbb{Z})$ . The set  $\rho(L)$  can be simultaneously diagonalized with diagonal entries being  $\pm 1$ . Now it is clear that  $d \geq k - \epsilon$ .  $\square$

A similar argument applies to  $F_i$  for all  $i \geq 2$  and show that the dimension of any complex representation of a finite quotient of  $A_{k+1}^+$  is at least  $k - \epsilon$ . Applying the main theorem proves the result.  $\square$

## REFERENCES

- [1] László Babai, Nikolay Nikolov, and László Pyber. Product growth and mixing in finite groups. In *Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 248–257, New York, 2008. ACM.
- [2] László Babai and Vera T. Sós. Sidon sets in groups and induced subgraphs of Cayley graphs. *European J. Combin.*, 6(2):101–114, 1985.
- [3] Hyman Bass and Alexander Lubotzky. *Tree lattices*, volume 176 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 2001. With appendices by Bass, L. Carbone, Lubotzky, G. Rosenberg and J. Tits.
- [4] Jean Bourgain and Alex Gamburd. Uniform expansion bounds for Cayley graphs of  $\mathrm{SL}_2(\mathbb{F}_p)$ . *Ann. of Math. (2)*, 167(2):625–642, 2008.
- [5] William Fulton and Joe Harris. *Representation theory*, volume 129 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.
- [6] W. T. Gowers. Quasirandom groups. *Combin. Probab. Comput.*, 17(3):363–387, 2008.
- [7] Ben Green and Imre Z. Ruzsa. Sum-free sets in abelian groups. *Israel J. Math.*, 147:157–188, 2005.
- [8] H. A. Helfgott. Growth in  $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$ . *J. Eur. Math. Soc. (JEMS)*, 13(3):761–851, 2011.
- [9] Kenneth Hoffman and Ray Kunze. *Linear algebra*. Second edition. Prentice-Hall Inc., Englewood Cliffs, N.J., 1971.
- [10] K. H. Hofmann and S.A. Morris. *The structure of compact groups*, volume 25 of *de Gruyter Studies in Mathematics*. Walter de Gruyter & Co., Berlin, augmented edition, 2006.
- [11] Kiran S. Kedlaya. Product-free subsets of groups. *Amer. Math. Monthly*, 105(10):900–906, 1998.
- [12] Vicente Landazuri and Gary M. Seitz. On the minimal degrees of projective representations of the finite Chevalley groups. *J. Algebra*, 32:418–443, 1974.
- [13] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.
- [14] N. Nikolov and L. Pyber. Product decompositions of quasirandom groups and a Jordan type theorem. *J. Eur. Math. Soc. (JEMS)*, 13(4):1063–1077, 2011.
- [15] Bryan P. Rynne and Martin A. Youngson. *Linear functional analysis*. Springer Undergraduate Mathematics Series. Springer-Verlag London Ltd., London, 2000.

- [16] Aner Shalev. Word maps, conjugacy classes, and a noncommutative Waring-type theorem. *Ann. of Math. (2)*, 170(3):1383–1416, 2009.
- [17] John S. Wilson. *Profinite groups*, volume 19 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, New York, 1998.

MOHAMMAD BARDESTANI, DÉPARTEMENT DE MATHÉMATIQUES ET STATISTIQUE, UNIVERSITÉ DE MONTRÉAL, CP 6128, SUCC. CENTRE-VILLE, MONTRÉAL, QC, CANADA H3C 3J7.  
*E-mail address:* bardest@dms.umontreal.ca

KEIVAN MALLAHI-KARAI, JACOBS UNIVERSITY BREMEN, CAMPUS RING I, 28759 BREMEN, GERMANY.  
*E-mail address:* k.mallahikarai@jacobs-university.de